MINISTRY OF EDUCATION OF THE REPUBLIC OF BELARUS

BELARUSIAN STATE UNIVERSITY

FACULTY OF INTERNATIONAL RELATIONS

Department of International Law

Annotation to the master's thesis

CYBERCRIME: THREATS TO BUSINESS AND COUNTERACTION AT THE INTERSTATE LEVEL

Zhao Xiqing

Scientific supervisor:

Borodulkina Yekaterina

Minsk, 2025

ANNOTATION

1. Structure and scope of the master's thesis: 49 pages, 3 chapters, 58 sources.

2. Keywords: cybercrime, business security, international cooperation, digital economy, cyber threats.

3. The content of the work

The object of the work is the legal relationships arising in connection with the commission of cybercrimes against business entities in the global digital economy.

The subject of the work includes the national legislation of various countries, international treaties, supranational regulations, court practice, and analytical reports of international organizations related to the prevention and control of cybercrime in the commercial sphere.

The purpose of this work is to deeply study and analyze the counteraction to cybercrime in the sphere of business, to study the legal experience of combating it at the international and national levels, as well as to develop proposals to improve the effectiveness of the fight against cybercrime, taking into account the mechanisms of international cooperation.

Research methods: the methodological basis of the research consists of the dialectical method for studying social and legal phenomena, as well as formal-logical methods such as deduction, induction, analysis, and synthesis. Private legal methods such as formal-legal, comparative-legal, and structural-legal analysis are also employed to assess different legal systems and international cooperation mechanisms in combating cybercrime.

Research results: The study systematizes the main types of cyber threats affecting businesses, identifies gaps and assesses the effectiveness of countering crime at various levels. The thesis proposes a multi-level model for countering cybercrime in the business sphere that systematically integrates international law, national strategies and corporate risk management practices. The study develops an approach to ensuring «business cyber resilience» that takes into account the need to create adaptive legal mechanisms in which criminal prosecution takes into account the intensity of technological evolution and the need to create corporate strategies that form the basis for sustainable and secure development of the digital economy.

Reliability of materials and results of the thesis: the study contains references to authoritative data sources to ensure the reliability and accuracy of the information. The work is based on an analysis of national and supranational legislation, international treaties and conventions, analytical reports and threat assessments by international organizations, academic literature, and court practice in significant cybercrime cases. The application of a range of scientific methods ensures the validity of the conclusions.

Recommendations for the use of the results: states are encouraged to update their criminal laws to keep up with the rapid development of new technologies, making sure the rules are tech-neutral and criminalizing new forms of illegal activity. International institutions and intergovernmental organizations should step up institutional cooperation under the new UN Convention on Cybercrime (2024). Commercial organizations are encouraged to implement integrated cyber resilience strategies, including proactive risk management systems. The scientific community is invited to focus its research on interdisciplinary analysis of challenges and responses to them.

АННОТАЦИЯ

1. **Структура и содержание магистерской диссертации:** 49 страницы, 3 главы, 58 источников.

2. Ключевые слова: киберпреступность, безопасность бизнеса, международное сотрудничество, цифровая экономика, киберугрозы.

3. Содержание работы

Объектом исследования являются правовые отношения, возникающие в связи с совершением киберпреступлений против субъектов хозяйственной деятельности в глобальной цифровой экономике.

Предметом работы являетя национальное законодательство различных стран, международные договоры, наднациональные нормативные акты, судебная практика, а также отчеты международных организаций, касающиеся предупреждения и борьбы с киберпреступностью в коммерческой сфере.

Цель данной работы – глубокое изучение и анализ противодействия киберпреступности в сфере бизнеса, изучение правового опыта борьбы с ней на международном и национальном уровнях, а также разработка предложений по повышению эффективности борьбы с киберпреступностью с учетом механизмов международного сотрудничества.

Методология исследования: состоит из диалектического метода изучения социальных и правовых явлений, а также формально-логических методов, таких как дедукция, индукция, анализ и синтез. Для оценки различных правовых систем и механизмов международного сотрудничества в борьбе с киберпреступностью также используются частноправовые методы, такие как формально-правовой, сравнительно-правовой и структурно-правовой анализ.

Результаты исследования: в исследовании систематизированы основные виды киберугроз, влияющих на бизнес, выявлены пробелы и оценена эффективность противодействия преступности на различных уровнях. В диссертации предложена многоуровневая модель противодействия киберпреступности в сфере бизнеса, которая систематически интегрирует международное право, национальные стратегии и корпоративные практики управления рисками. В исследовании разработан подход к обеспечению «киберустойчивости бизнеса», учитывающий необходимость создания адаптивных правовых механизмов, в которых уголовное преследование учитывает интенсивность технологической эволюции, а также необходимость создания корпоративных стратегий, формирующих основу для устойчивого и безопасного развития цифровой экономики.

Надежность материалов и результатов диссертации: исследование содержит ссылки на авторитетные источники данных для обеспечения надежности и точности информации. Работа основывается на анализе национального и наднационального законодательства, международных

договоров и конвенций, аналитических отчетов и оценок угроз международных организаций, академической литературы и судебной практике по значимым делам о киберпреступлениях. Применение комплекса научных методов обеспечивает обоснованность выводов.

Рекомендации по использованию результатов: государствам рекомендуется модернизировать уголовное законодательство с учетом интенсивного развития новых технологий, обеспечив технологическую нейтральность норм и криминализацию новых форм противоправной деятельности. Международным институтам и межправительственным организациям следует активизировать институциональное сотрудничество в рамках Конвенции ООН против киберпреступности (2024). Коммерческим организациям рекомендуется внедрение интегрированных стратегий киберустойчивости, включающих проактивные системы управления рисками. Научному сообществу предлагается сфокусировать исследования на междисциплинарном анализе вызовов и ответов на них.